MIT 6.042J HW1 2005

Kelly Lin

June 2019

1 Problem 1

Prove that $\sqrt[3]{2}$ is not sensible.
I will be doing a proof by contradiction.
Let us assume that $\sqrt[3]{2}$ is sensible. We will set it equal to $\sqrt{\frac{a}{b}}$.
We square both sides, then cube both sides to get

$$\frac{a}{b} = \sqrt[3]{4}$$

This implies that $\sqrt[3]{4}$ is a rational number. Rational numbers can be written as a fraction in lowest terms where the numerator and denominator are both integers.

$$\frac{x^3}{y^3} = 4$$
$$x^3 = 4y^3$$

$4y^3$ must be even because 4, an even number, multiplied by anything turns it even.

x^3 must be even because the right side was even.

x itself must be even because of that. Then x^3 must be divisible by 8.
That means that $4y^3$ must also be divisible by 8.

Since the 4 isn't enough to cover 8, y^3 must also be divisible by 2, therefore even.

Then y must be even.

If both x and y are even then they are not in lowest terms.
This contradiction means that $\sqrt[3]{4}$ isn't rational.

Since it being sensible implied that it was rational, it can't be sensible.

2 Problem 2

"There is a student who has emailed exactly two other people in the class, besides possibly herself." Okay, so we know there's three students here. I'll call them s, t, and u.

$$\exists s \exists t \exists u \in S$$

s has emailed t and s has emailed u.

$$E(s,t) \land E(s,u)$$

s is a different student from u, and a different student from t, and same goes for u and t.

$$s \neq u \land s \neq t \land u \neq t$$

Of the students that s has emailed, those students are either u, t, or themselves. So we can say "Every student o that s has emailed, o is equal to s, t, or u."

$$\forall o \in SE(s,o) \to o = s \lor o = t \lor o = u$$

So we can AND all of the phrases together to make the predicate.

$\exists s \exists t \exists u \in S.E(s,t) \land E(s,u) \land s \neq u \land s \neq t \land u \neq t \land \forall o \in S.E(s,o) \to o = s \lor o = t \lor o = u$

3 Problem 3

Write in predicate form. Addition, multiplication, equality, but no constants. Prove stuff first before using. This is over the domain of the natural numbers (non-negative integers).

a. n is the sum of three perfect squares

$$\exists x \exists y \exists z.x * x + y * y + z * z = n$$

I don't have to specify anything special on these since it's fine if x, y, and z are the same as each other.

b. x > 1

Since we can't use constants, we need to first define $x = 1$.

$$\forall y.(y * x = y)$$

Now we can set things equal to one using the above definition.

$$\exists y.(x > y) \wedge (y = 1)$$

Kind of confused on who takes the exists in the above line.

c. n is a prime number.

Well, I know that it isn't possible to have two variables that multiply each other to become n.

$$\neg(x * y = n)$$

Also have to declare it. So it's more like...

$$\neg(\exists x \exists y.(x > 1 \wedge y > 1 \wedge x * y = n))$$

And we know that n, the prime number, has to be bigger than 1. So altogether:

$$IS - PRIME(n) ::= (n > 1) \wedge \neg(\exists x \exists y.(x > 1 \wedge y > 1 \wedge x * y = n))$$

d. n is a product of two distinct primes.

$$\exists a \exists b.IS - PRIME(a) \wedge IS - PRIME(b) \wedge \neg(a = b) \wedge (a * b = n)$$

e. There is no largest prime number.

So we're going to want to do a NOT on the statement "There is a largest prime number." To say that there is a largest prime number, we want to specify that 1. there exists a p where IS-PRIME(p) and 2. for all q where q is a prime number, that it follows that there is a p bigger than or equal to q. So let's see about the first statement...

$$\exists p.IS - PRIME(P)$$

And the second statement:

$$\forall q.IS - PRIME(q) \rightarrow p \leq q$$

And then we want to AND those two together and then NOT the whole thing.

$$\neg(\exists p.IS - PRIME(P) \wedge (\forall q.IS - PRIME(q) \rightarrow p \leq q))$$

f. Goldbach conjecture. Every even natural number $n > 2$ can be expressed as the sum of two primes.

This is a combo of a couple of statements. We need to explain what an even number is. We need to explain what it means for something to be bigger than 2. This requires us to define how something can be equal to 1 (which we did do back up in problem 3b). Then we can make use of the IS-PRIME function and link it all together with a right arrow "implies".
This is the definition of 1:

$$\forall y.(y * m = y)$$

This is the definition of a thing to be bigger than 2:

$$\exists y.(y = 1) \wedge (x > y + y)$$

This is the definition of an even number:

$$\forall y.(x = 2y)$$

So pulling it together:

$$\forall n.((n > 2 \wedge \exists y.n = 2y) \rightarrow \exists p \exists q.IS - PRIME(p) \wedge IS - PRIME(q) \wedge (n = p + q))$$

g. Bertrand's Postulate. If $n > 1$ then there is always at least one prime p such that $n < p < 2n$.

Since we have already shown how to have a variable be less than another variable, how a thing can be prime, we can simply write:

$$\forall n.(n > 1) \rightarrow \exists p.IS - PRIME(p) \wedge (n < p) \wedge (p < 2n)$$

4 Problem 4

I will be doing a proof by contradiction.
So a surjection is a function where every single element of the y result (codomain) is mapped to by at least one element of the x input (domain).
Let's say there is a surjective function (aka surjection) $f : A \to P(A)$, where P is the powerset.
Making use of that helpful hint, let's define a set S where:

$$S ::= x \in A | x \notin f(x)$$

Looking at that first part of the definition, this means that if an x belongs to S, then it must not be in f(x):

$$(x \in S) \leftrightarrow (x \notin f(x))$$

Because x is an element that belongs to set A, by definition S must be a subset of A. If $S \subseteq A$, then S must also be in the powerset of A, P(A). So S must equal f(a) for an $a \in A$.

$$(x \in f(a)) \leftrightarrow (x \notin f(x))$$

If we plug in x for a in the above equation, it's a contradiction.

$$(x \in f(x)) \leftrightarrow (x \notin f(x))$$

Can't be both in it and not in it at the same time. Therefore if A is infinite, there still does not exist a surjection f from A to its powerset P(A).

5 Problem 5

a. I don't completely understand this problem. It says to prove that

$$\exists z.[P(z) \wedge Q(z)] \to [\exists x.P(x) \wedge \exists y.Q(y)]$$

If there exists a z where we have a function that acts on z and a different one that acts on z...I guess it follows that there exists an x where that same function acts on x, and then there exists a y where that same second function acts on y, because there's nothing restricting the x and y from being z if we're in the same domain, right? It feels like we're saying something super fundamental and it's hard to know how to describe it.

The problem set official solution says that we assume

$$\exists z.[P(z) \wedge Q(z)]$$

That it holds for some element z in the domain. It then says to let c be this element, so that we have:

$$[P(c) \wedge Q(c)]$$

Then it says the first term there holds by itself.

$$P(c)$$

By Existential Generalization, there exists an x where:

$$\exists x.P(x)$$

Apparently, we can say the same of that second term:

$$Q(c)$$

And then the y:

$$\exists y.Q(y)$$

Hence, that original conclusion we were looking at holds.

$$\exists x.P(x) \wedge \exists y.Q(y)$$

b. Prove that the converse is not valid by describing a counter model.

Okay, so in the above there was an expression implying another expression, which maybe I can call the first expression left-hand-side and the second expression right-hand-side. We showed that LHS implied RHS. So if LHS is true, RHS is also true and cannot be false. Just looking at that original predicate (is that the right term?), since the arrow was only going one direction, if LHS was false then RHS could still be either true or false.

Now thinking about the converse...the converse of that original predicate is that RHS implies LHS. So the converse would assert that if RHS is true, LHS cannot be false. Let's describe a counter model that has a case where RHS is true but LHS is false. Here's the converse:

$$\exists x.P(x) \wedge \exists y.Q(y) \rightarrow \exists z.[P(z) \wedge Q(z)]$$

Let's say the domain is [1, 3]. Inclusive between 1 and 3, and let's say it has to be integers. So we want to say that the following expression is true:

$$\exists x.P(x) \wedge \exists y.Q(y)$$

So let's say that the function P just takes the input and checks if the input is equal to 1. So if x is equal to 1 then P(x) is true. And let's say that the function

Q takes the input and checks if the input is equal to 3. So if x is equal to 3 then Q(x) is true. We can see then that in the case of x being 1 and y being 3, that P(x) and Q(y) are then true.

However, that other expression:

$$\exists z.[P(z) \land Q(z)]$$

Is now false. Because z can only be 1, 2, or 3, and whichever one it is, it'll fail one or more of the functions. Hence the converse is not true.

6 Problem 6

a. Give an example where the following result fails (see problem set).

The False Theorem fails when A and D are empty sets, and C and B are nonempty sets. L becomes C X B and R becomes zero.

b. Identify the mistake in the following proof.

The mistake is with the third line to the fourth line of the proof. It states that for L:

$$(x \in A \lor x \in C) \land (y \in B \lor y \in D)$$

if and only if R:

$$(x \in A \land y \in B) \lor (x \in C \land y \in D)$$

But these two expressions are NOT equivalent. If we flip L to be in the same "format" that R is written in, L becomes:

$$(x \in A \land y \in B) \lor (x \in A \land y \in D) \lor (x \in C \land y \in B) \lor (x \in C \land y \in D)$$

So you can see that L encompasses more things than R. R is more restrictive.

c. Fix the proof to show that $R \subseteq L$

The if and only if after the third line's expression can be changed to if. Iff is bidirectional in the implication, whereas here, the third line will be true if the fourth line is true, since the fourth line is more stringent. So it's like fourth line implies the third line, but third line does not imply the fourth line.

The problem set official solution says to say "which will be true when", which does seem a bit clearer than just an if.